


Havells India

Incident Management Policy

Version 1.0

Havells India Limited Havells India Incident Management Policy Version 1.0 Internal	
--	---

Document Approvers

Sr. No.	Type of Information	Document Data
a.	Document Title	Havells India Incident Management Policy
b.	Document Code	HIMP
c.	Date of Release	20th Feb 2023
d.	Document Superseded	
e.	Document Approvers	Mr. Pramod Mundra and Mr. Ramanand Jha
f.	Document Owner	Information Security Head
g.	Documents Author(s)	Mr. Sanjay Roongta and Mr. Neeraj Nagpal

Document Approvers

S. No.	Approver	Approver Designation	Approver Contact
1.	Pramod Mundra	Chief Information Officer (CIO)	Pramod.Mundra@havells.com
2.	Ramanand Jha	Information Security Head (ISH)	ramanand.jha@havells.com

Document Change Approvals

Version No	Revision Date	Nature of Change	Date Approved
1.0	NA	Initial Version	18th Feb 2022
1.0	NA	No change	17th Feb 2023

Havells India Limited Havells India Incident Management Policy Version 1.0 Internal	 HAVELLS
--	---

Document Scope

The scope of Incident Management Policy covers the incidents impacting the IT infrastructure and IT applications of Havells.

Document Distribution

The Information Security Head (ISH) shall distribute this policy to all employees working with IT department and/or handling, processing, and managing information/information assets of Havells by uploading it on the intranet/by sharing it via email/as appropriate.

Document Conventions

All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

Table of Contents

1. Purpose	5
1.1 Scope	5
1.2 Responsibility.....	5
1.3 Enforcement	5
1.4 Authority	5
2. Policy.....	5
2.1. Overview	5
2.2. Incident Life Cycle	6
2.3. Reporting of Incidents.....	6
2.4. Incident logging and categorization & prioritization.....	6
2.5. Initial Investigation and Diagnosis	7
2.5.1. Initial Investigation	7
2.5.2. Diagnosis and Support	8
2.6. Resolution and Recovery	8
2.7. Incident Closure	9
2.8. RACI Matrix for Incident Lifecycle	9
2.9. Information Security Incident Management	10
2.9.1. Reporting security incidents.....	10
2.9.2. Incident Prioritization	11
2.9.3. Incident Investigation and Diagnosis	12
2.9.4. Incident Resolution and Recovery	12
2.9.5. Learning from the Security incidents	13
2.10. RACI Matrix for Security Incident Lifecycle	13
2.11. Post Incident Review	14
2.12. Problem Management	14
2.13. Collection of Evidence	16

<p>Havells India Limited</p> <p>Havells India Incident Management Policy</p> <p>Version 1.0</p> <p>Internal</p>	
---	---

1. Purpose

This policy intends to establish guidelines for early detection, reporting and resolution of incidents, to reduce the risks presented because of these incidents.

1.1 Scope

The scope of Incident Management Policy covers the incidents impacting the IT infrastructure and IT applications of Havells.

1.2 Responsibility

It is the responsibility of the IT Team and respective or concerned business/functional team to implement and maintain the guidelines as defined in this policy.

1.3 Enforcement

All incidents impacting the IT infrastructure and IT applications of Havells are covered under this policy. Requests for deviations from this policy must be documented and managed using the approved process. Any deviations from this policy must be approved in accordance with the Security Exception Management Policy.

1.4 Authority

The Chief Information Officer (CIO) and Information Security Head (ISH) approves and enforces this policy and mandates processes to monitor and ensure compliance to this policy.

2. Policy

2.1. Overview

This policy intends to establish guidelines for early detection, reporting and resolution of incidents, to reduce the risks presented because of these incidents. This policy ensures that untoward events associated with information assets (Example: applications, data, paper or electronic documents, hard drive, laptop, server, backup tapes, etc.), physical security and other business / Information Technology (IT) operations are communicated and managed in a manner allowing timely corrective action to be taken. The policy establishes a consistent and effective approach to the management of incidents within Havells.

The goal of incident management is to restore the normal service operations and to minimize the adverse impact on the business operations thus ensuring that the best possible levels of service quality and availability of service is maintained.

The primary objectives of incident management shall be following, but not restricted to:

- a) To early detection, reporting and resolution of incidents;
- b) To devise and apply a consistent approach for incident management;
- c) To log, manage and track incidents;

- d) To maintain records/logs pertaining to incidents;
- e) To align incident management activities and priorities with those of the business; and
- f) To gather learnings/knowledge from the incidents to proactively avoid reoccurrence in future

2.2. Incident Life Cycle

The below mentioned workflow represents the phases involved for handling an incident:

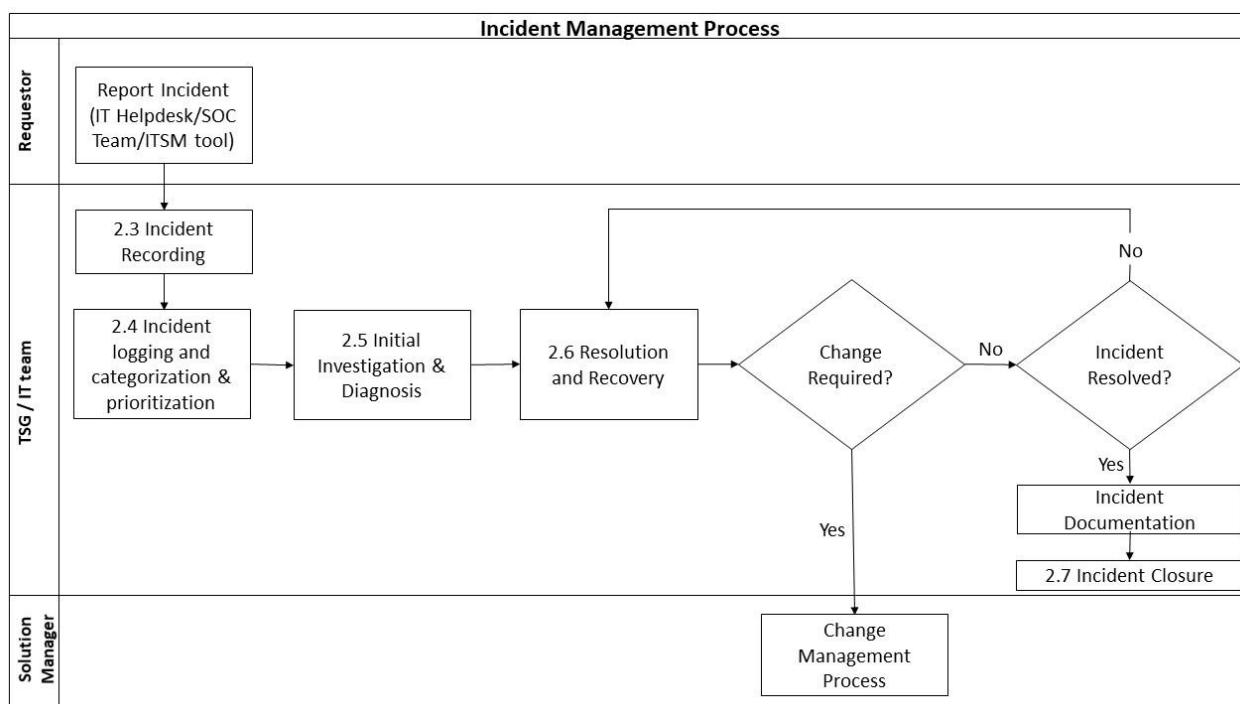


Table 1 Incident Management Process

2.3. Reporting of Incidents

Incidents can be reported through the below mentioned channels:

- a) Logging a call on 0120-477-2399;
- b) Writing to ITsupport.Helpdesk@Havells.com; and
- c) Logging an incident on the ITSM tool.

All the incidents reported via call and e-mail are logged in the ITSM tool

2.4. Incident logging and categorization & prioritization

Incidents shall be logged and categorized & prioritized to ensure effective and efficient handling of incidents. Prioritization is imperative to ensure that appropriate focus and precedence is given to incidents based on their priority.

Priority	Definition	Severity	Impact	Response Time	Resolution Time
VVIP	Senior management / leadership user tickets. An incident or events where the impact to the business is deemed critical or high severity	Critical	Impact >=1 user	10 minutes	<=1 hour
P1	One or more business critical application(s)/ service(s) is down for all the locations	Critical	Impact >50% to 100% users	10 minutes	<=1 hour
P2	An incident where the impact to system operations is limited to a small area, or where one or more business critical application down.	High	Impact >20% and <50% users	30 minutes	<=2 hours
P3	An incident which has localized scope and low impact or an event where a single user is affected.	Medium	Impact <=1 user	45 minutes	6 hours
P4	An incident that cannot directly impact system operations, and can be contained by compensating controls	Low	No direct impact on users	60 minutes	<=16 hours

Table 2 Incident prioritization

2.5. Initial Investigation and Diagnosis

Initial investigation and Diagnosis consist of two stages:

2.5.1. Initial Investigation

There are two teams involved in the initial investigation:

- a) Helpdesk Team: The Helpdesk team shall be responsible for probing and capturing the needed information to perform necessary troubleshooting activities. Helpdesk team shall perform the following activities, but not limited to:
 - i. Handle the user calls, emails & tickets;
 - ii. Be responsible for end to end case ownership;
 - iii. Report effective probing of issue; and
 - iv. Assign case to the relevant resolver groups;
- b) IT Support Team: IT Support Team shall be responsible for carrying out initial investigation and providing first level support for incidents that are within their purview. Initial investigation shall be carried out to identify symptoms of the issue to determine what exactly has gone wrong and how it can be rectified. IT support analysts shall perform following activities, but not limited to:
 - i. Probing questions information;
 - ii. The available diagnostic scripts; and

<p style="text-align: center;">Havells India Limited Havells India Incident Management Policy Version 1.0 Internal</p>	
---	---

- iii. Knowledge Base Articles (KBA) and the Known Error Database (KEDB) to perform initial diagnosis and to render first level support;
- c) All the information collated, and steps taken during this phase must be captured in the incident record;
- d) If a resolution is identified for the incident at this point, the process flows to Resolution and Recovery;
- e) If the incident is not within the scope of IT support or if it is not resolved after initial troubleshooting and support, it shall be assigned to the relevant Technical Specialist Group (TSG) for further investigation, diagnosis, and support;
- f) Incident Assignment & Acceptance: Incidents shall be assigned to the appropriate Technical Support Group by Helpdesk for expert support in case first (Helpdesk) and second (IT Support) level support is unsuccessful or not applicable;
- g) The Technical Support Group to whom the incident is assigned shall review the incident record and confirm whether they are the correct expert support group who are required to resolve the incident; and
- h) The assigned group shall assume ownership of the incident and begin investigation if the assignment is deemed to be accurate. On the other hand, if it is determined that the incident has been incorrectly assigned to a support group, they shall reroute the incident to the right support group or to Helpdesk for correct assignment.

2.5.2. Diagnosis and Support

- a) Diagnosis and Support can be iterative in nature with multiple interactions between the Helpdesk, Support Groups, and end users for information/action;
- b) Support Group Specialists from the assignment group shall embark on detailed investigation and diagnosis in a bid to resolve the incident and restore normal service operation;
- c) This may include the utilization of advanced technical scripts, diagnostic tools and utilities and specific Knowledge Base Articles accessible to expert support groups;
- d) If required, Third Party vendors and external subject matter experts may also be roped in; and
- e) All activities and steps taken during the Diagnosis and Support phase shall be documented in the incident record to provide a complete account of events.

2.6. Resolution and Recovery

- a) The objective of the Resolution and Recovery phase is to test and apply identified resolutions to recover from the incident;
- b) If a change is required to resolve the incident, changes shall be routed to change management process; and
- c) Resolution and Recovery runs parallel with Diagnosis and Support so that any potential resolutions identified can be immediately implemented, thereby improving service restoration.

2.7. Incident Closure

- This phase of the Incident Management Process commences once the status of an incident has been set to 'Resolved';
- The incident shall be closed upon resolution acceptance by the requester or it will be closed automatically in case the requester does not respond within 24 business hours;
- Once an incident is set to 'Closed' status, it is completely frozen and cannot be edited or reopened under any circumstances; and
- In case the requester rejects the resolution, the incident will be reassigned to the Support Group who had resolved the incident to review the situation and provide an acceptable resolution.

2.8. RACI Matrix for Incident Lifecycle

Incident shall be monitored and tracked throughout the incident lifecycle, from detection to closure. The table below defines where ownership lies in various teams:

Incident Lifecycle	Helpdesk Team	IT Support Group	Technical Support Group	Security Team	End Users
Incident reporting	R, A	R	R	R, I	R, A
Incident logging and categorization & prioritization	R, A	R	R	I	I
Initial investigation	I	R, A	C		I
Diagnosis and Support	I	R, A	R, A	C	I
Resolution and Recovery	I	R, A	R, A		I
Incident Closure	I	R, A	R, A	I	I

R- Responsible A- Accountable C- Consulted I- Informed

Table 3 RACI Matrix for incident lifecycle

The resolution ownership of incidents lies with the Support Group to whom the incident is assigned, and the incident assignee shall be the resolution owner for a given incident.

The resolution owner shall be responsible for the following activities, but not restricted to:

- Incident investigation and diagnosis;
- Developing workarounds and solutions;
- Provide timely technical updates to the Solution Manager / operations lead in case of a critical incident;
- Engage Third Party vendors and subject matter experts as and when required;

- e) Document complete details of the resolution along with the appropriate resolution code; and
- f) Creation, assignment, and communication of incident tasks to other support groups if necessary.

2.9. Information Security Incident Management

Information security incident management details handling of potential information security event through the investigation and evaluation process to ensure that information security incidents are addressed in a timely and effective manner and in accordance with Havells' Information Security Policy, procedures, and legal requirements. When necessary, procedures for the timely notification to employees, and all other parties who may be impacted by the incident are initiated, and appropriate remedial actions are taken.

The objectives of Information security incident management are as follows:

- a) Ensure that information security events and vulnerabilities associated with information systems are communicated in a manner allowing timely corrective actions to be taken;
- b) Ensure that a consistent and effective approach is applied to the management of information security incidents

Havells must be prepared to deal with numerous types of information security related events and incidents, including Denial of Service (DoS) attacks, malicious code/ malware infection, unauthorized access, inappropriate usage (violating acceptable use policies), and data breaches (an incident in which confidential data is lost or stolen; the integrity of confidential data is/ was affected; confidential data was/ is subject to unlawful disclosure).

In order to protect Havells' network and the information stored and processed, Havells' network must have consistent processes for reporting, tracking, and managing security events and incidents. This includes defining how Havells' network will respond when it is notified of a potential security event and incident.



Table 4 Steps involved in information security incident management

2.9.1. Reporting security incidents

- a) All information security incidents must be reported at:
 - i. Email: soc@havells.com / ITsupport.Helpdesk@Havells.com; and
 - ii. Report it through telephone via IT Helpdesk at: 0120-477-2399.
- b) Employees shall be made aware of their responsibilities for reporting information security event and incidents;

<p>Havells India Limited</p> <p>Havells India Incident Management Policy</p> <p>Version 1.0</p> <p>Internal</p>	
---	---

- c) Where it is required to report information security incidents to outside authorities to comply with legal or regulatory requirements, this shall only be done by ISH/matrix approved by ISH;
- d) All the suspected/potential/detected/actual incidents shall be reported. Such incidents shall include, but not limited to:
 - i. Any data breach, loss of data/ information, intellectual capital, software, or physical assets (or confidential information), transfer to an unauthorized recipient, including, for example, information on laptops, smart-phones, USB devices, documents and working papers;
 - ii. If any Havells personnel believe that their credentials may have been compromised or lost, or in the event that access device is lost or stolen;
 - iii. Any actual or suspected malware infection causing potential disclosure of information or loss of control of the device;
 - iv. Any violation of the Acceptable Usage Policy; and
 - v. Any identified information security weaknesses and vulnerabilities (under no circumstances should any Havells personnel or Third-Party attempt to test or exploit an identified weakness or vulnerability unless it is within their job responsibility to do so).

2.9.2. Incident Prioritization

Information Security Incident handling shall be prioritize based on the following guidelines:

- a) **Current and Potential Technical Impact, likelihood of the Incident:** Incident handlers should consider not only the current negative impact of the incident (For example: unauthorized user-level access to data), but also the likely future technical impact of the incident if it is not immediately contained (For example: root level compromise). For example, a malware spreading among workstations may currently cause a minor effect on the business operations, but within a few hours, the malware's 's impact on network traffic may cause a major network outage; and
- b) **Criticality of affected Resources and/or Information Assets:** Resources affected by an incident (For example: firewalls, web servers, Internet connectivity, user workstations, and applications etc.) have different significance to different business operations. The criticality of a resource is based primarily on its information or services, users, trust relationships and interdependencies with other resources, and visibility (For example: a public web server / E-com Portal versus an internal web server).





Priority	Definition	Severity	Impact	Response Time	Resolution Time
 VVIP	An actual or suspected security incident which might have impact on any leadership user's system.	Critical	Impact >=1 user	10 minutes	<=1 hour
 P1	An actual or suspected security incident which might have high to medium business impact.	High	Impact >=1 user	10 minutes	<=1 hour
 P2	A suspected or potential security incident which might have medium business impact.	Medium	Impact >=1 user	30 minutes	<=2 hours
 P3	A suspected or potential security incident which might have low business impact.	Low	Impact <=1 user	45 minutes	6 hours

Table 5 Information security incident prioritization

2.9.3. Incident Investigation and Diagnosis

- a) Investigation:
 - i. Security incidents shall be investigated, analyzed, and preventive and corrective actions shall be taken to minimize recurrence of the incident; and
 - ii. Investigation shall be carried out based on the Priority
- b) Diagnosis:
 - i. Identifying root cause analysis of the incident along with corrective actions to be taken by the identified stakeholders, to avoid recurrence of the incident; and
 - ii. Based on the outcome of the action taken, IT Team shall provide the status report of the incident to ISH/Head of IT/CIO

2.9.4. Incident Resolution and Recovery

Appropriate actions shall be taken as per the defined Incident Management process to further contain any impact on IT services. This may include actions such as disconnection of IT systems from network, strengthening controls on access to sensitive information, e-mail & internet transactions, restricting access to internet sites, intrusion detection systems to prevent network attacks, collection of genuine incident related transaction trails from end-users etc.

- a) Perform recovery activities to return impacted assets to an operational state with appropriate security controls (e.g., hardening, monitoring, and/or patching improvements);
- b) Test and monitor the recovered assets and related systems to ensure they are operational, returned to operating conditions, and that eradication efforts have been maintained (e.g., that a malicious user has not re-exposed the asset(s) or undone the remediation efforts);
- c) Once testing and monitoring are completed, make an assessment to determine if security-related recovery actions were successful;
- d) Ensure the validation of the security state of Havells' network has been maintained beyond initial eradication efforts by monitoring for re-occurrence of the security incident; and
- e) Communicate outcomes to key stakeholders.

2.9.5. Learning from the Security incidents

- a) Learnings shall be analysed to identify security risks and process enhancement opportunities. A knowledge base shall be referred to for incident handling and as a learning source of information security incidents.
- b) User awareness sessions/Mock Drills shall be conducted for both IT Teams (who deal with confidential data) and non- IT users towards their roles and responsibilities in dealing with security incidents throughout the incident lifecycle;
- c) Learning from security incidents shall be leveraged for enhancing security training and awareness program in Havells; and
- d) The learning from evaluation of information security incidents shall be communicated to all employees.

2.10. RACI Matrix for Security Incident Lifecycle

Security incident shall be monitored and tracked throughout the security incident lifecycle, from detection to closure. The table below defines where ownership lies in various teams:

Security Incident Lifecycle	Helpdesk Team	IT Support Group	Technical Support Group	Security Team	ISH	CIO	End Users
Reporting Security Incidents	R, A	R	R	R, A, I	R, I	R, I	R
Security Incident Prioritization	R, A			R, A	C	I	I
Security Incident Investigation and Diagnosis	I		C	R, A	C, I	C, I	I
Security Incident Resolution and Recovery	I		C	R, A	R, C	C, I	I

Security Incident Lifecycle	Helpdesk Team	IT Support Group	Technical Support Group	Security Team	ISH	CIO	End Users
Post Incident Review	I	I	C, I	R, A	I	I	I

R- Responsible A- Accountable C- Consulted I- Informed

Table 6 RACI Matrix for information security incidents

2.11. Post Incident Review

- A formal Post Incident Review (PIR) shall be carried out for P1 (both non-security and Security incidents) to ensure that any weaknesses in systems, processes and procedure are identified and rectified by performing a Root Cause Analysis (RCA). The PIR shall be carried out by the Incident Response Team who handled the incident;
- A Post Incident Review shall be schedule by IT Team to ascertain the efficiency of security controls (preventive/detective) to avoid recurrence of the incident. Further, RCA shall be documented for identified incidents; and
- IT Team at Havells shall establish a knowledge base for the information gained from the post incident reviews.

2.12. Problem Management

Problem Management seeks to minimize the adverse impact of Incidents by preventing Incidents from happening. For Incidents that have already occurred, Problem Management tries to prevent these Incidents from happening again. Problem Management increases stability and integrity of the infrastructure.

The objective of Problem Management is to minimize the impact of Incidents on the IT Infrastructure, applications, and the business by identifying root cause, logging known errors, providing and communicating workarounds, finding permanent solutions, and preventing recurrence of incidents related to these errors.

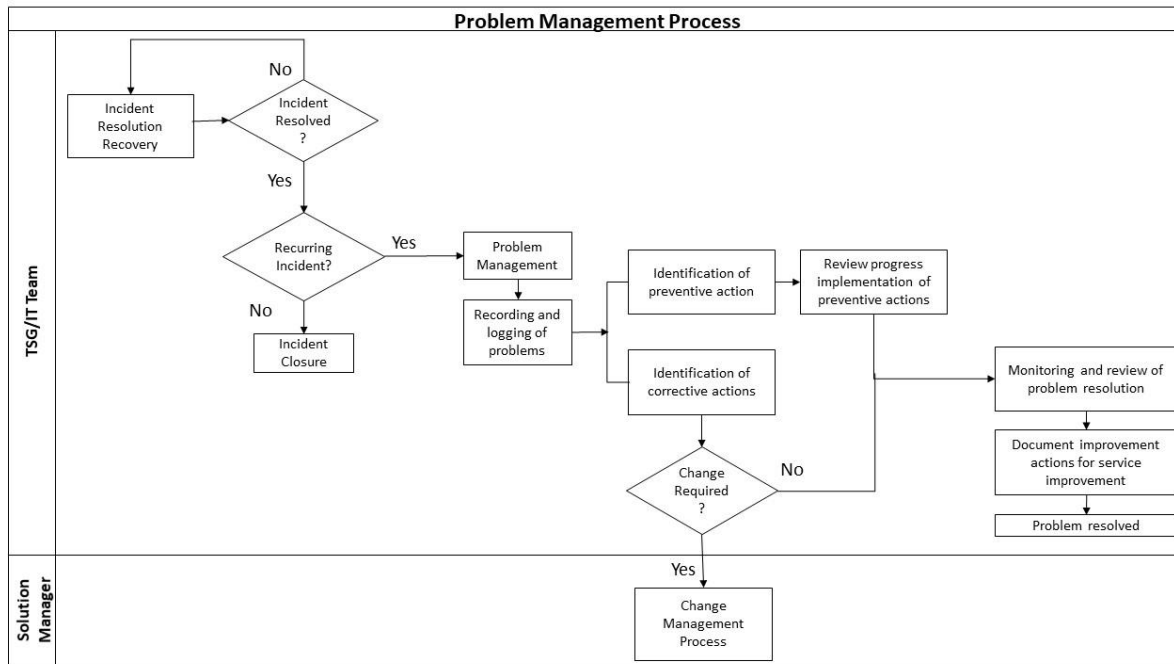


Table 7 Problem Management Process

Effective Problem Management requires the identification and classification of problems, Root Cause Analysis (RCA) and resolution of problems. A problem shall be classified as known error once the root-cause and a workaround are available. Known errors identified through RCA shall be available in the knowledge database.

- All the identified problems shall be recorded and classified based on the impact to business;
- All problems shall be updated on the progress till resolution and closure;
- Preventive action shall be identified to reduce potential problems based on repeat incident analysis and proactive management;
- Work around shall be provided wherever possible to reduce or eliminate the impact of the problem on business;
- There shall be defined reports and review schedules for the closed and pending/open problems respectively;
- Any corrective actions and problems requiring changes from an end user perspective shall be resolved through change management process;
- Problem resolution shall be monitored, reviewed, and reported for its effectiveness; and
- Actions for improvement identified shall be recorded and form an input to the service improvement plan.
- Where actions for Information Security related problem management should be reviewed with ISH before execution

<p>Havells India Limited</p> <p>Havells India Incident Management Policy</p> <p>Version 1.0</p> <p>Internal</p>	
---	---

2.13. Collection of Evidence

Where a follow-up action against a person or organization after an information security incident involves legal action, (either civil or criminal) evidences shall be collected, maintained, and presented to the relevant authorities as per the company policy / DOA.